Hepting et al v. AT&T Corp. et al Doc. 264

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (Bar No. 145997)
cindy@eff.org
LEE TIEN (Bar No. 148216)
tien@eff.org
KURT OPSAHL (Bar No. 191303)
kurt@eff.org
KEVIN S. BANKSTON (Bar No. 217026)
bankston@eff.org
CORYNNE MCSHERRY (Bar No. 221504)
corynne@eff.org
JAMES S. TYRE (Bar No. 083117)
jstyre@eff.org
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

Attorneys for Plaintiffs

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL and ERIK KNUTZEN, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, vs. AT&T CORP., et al. Defendants.	No. C-06-00672-VRW CLASS ACTION PLAINTIFFS' OPPOSITION TO MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT BY THE UNITED STATES OF AMERICA BASED ON THE STATE SECRETS PRIVILEGE Judge: The Hon. Vaughn R. Walker Date: June 23, 2006 Courtroom: 6, 17th Floor

REDACTED PUBLIC VERSION

Dockets.Justia.com

TABLE OF CONTENTS

Page

INTRODUCTION 1

STATEMENT OF FACTS 5

The Creation Of The [redacted] Room 5

NSA Control Of The [redacted] Room 5

The Communications Diverted To The [redacted] Room 6

The Capabilities Of The Equipment In The [redacted] Room 7

The [redacted] Backbone Network 7

AT&T's Other [redacted] Rooms 8

Warrantless Surveillance By The Government Using AT&T Facilities 8

ARGUMENT 9

I. THE STATE SECRETS PRIVILEGE DOES NOT WARRANT DISMISSAL ABSENT EXTRAORDINARY CIRCUMSTANCES NOT PRESENT HERE 9

A. The State Secrets Privilege Does Not Provide The Basis For Dismissing This Case 9

1. The State Secrets Privilege Does Not Confer Immunity 10

2. The Exceptional Authority To Dismiss A Case Where Its Subject Matter Is A State Secret Does Not Exist Here 12

B. Congress Has Limited The State Secrets Privilege In The Context Of Electronic Surveillance 16

1. Congress Has The Power To Limit The Government's Ability To Invoke The State Secrets Privilege 16

2. Congress Has Directly Spoken To The Application Of The State Secrets Privilege In Electronic Surveillance Cases 17

a. Congress created private rights of action to enforce strict rules governing electronic surveillance 18

b. Congress provided for disclosure of the existence of electronic surveillance through "legal process" 20

c. Congress provided for discovery of classified materials pertinent to the legality of the surveillance in 50 U.S.C. §§ 1806(f) and 1845(f) 21

TABLE OF CONTENTS

Page

d. The government cannot manufacture immunity from the statutory disclosure requirements by disregarding FISA altogether....23

3. Congress' General Directives To The NSA Do Not Change The Procedure For Discovery Regarding Electronic Surveillance....24

C. The State Secrets Privilege Cannot Permit Dismissal Of Claims Seeking Relief From Ongoing Violation of Constitutional Rights....26

II. PLAINTIFFS' CLAIMS CANNOT BE DISMISSED ON THE GROUNDS OF THE STATE SECRETS PRIVILEGE BECAUSE THEY ARE BASED ON NON-SECRET INFORMATION....28

A. The State Secrets Privilege Does Not Change the Standard of Review....28

B. The Government Cannot Retroactively Transform Non-Secret Information Into A State Secret....29

1. Plaintiffs' Interception Claims....31

a. Count III – Violation of 18 USC §2511....31

b. Count II – Violation of 50 U.S.C. §§ 1809-10....32

2. Plaintiffs' "Divulgence/Disclosure Claims"....34

a. Count III – 18 U.S.C. §§ 2511(1)(c), (d), and (3)(a)....34

b. Counts V and VI – The Stored Communications Act (18 U.S.C. § 2702(A))....36

C. The Constitutional Claims....37

1. The Constitution Requires That The Government Obtain A Warrant Based On A Particularized Showing Of Probable Cause....38

2. No Exception To The Warrant Requirement Exists In This Case....40

a. The purported "foreign surveillance" exception, which has not been recognized by the Supreme Court, is inapplicable....40

b. The "special needs" exception is inapplicable....42

3. Proving AT&T's Violation Of The Fourth Amendment Does Not Require Probing State Secrets....44

a. The evidence establishes a violation of the warrant requirement....44

TABLE OF CONTENTS

Page

b. AT&T's actions as an agent of the government are not protected by the state secrets privilege 44

III. THE ALLEGED SECRET CERTIFICATION DEFENSE DOES NOT PROVIDE THE BASIS FOR DISMISSING THIS CASE..45

A. "Secret Certifications" Would Eliminate The Private Rights Of Action Created By Congress...46

B. Title 18 U.S.C. § 2511(2)(a)(ii) Provides For Disclosure Of Certifications Where The Underlying Surveillance Has Been Established Using Non-Classified Evidence..47

C. The Certifications Cannot Be Classified As A "Secret" For Purpose Of Maintaining the Secrecy Of AT&T's Surveillance Activities When Such Activities Are Already Established By Record Evidence.....................................48

IV. STANDING CAN BE ESTABLISHED WITHOUT IMPLICATING FACTS PROTECTED BY THE STATE SECRETS PRIVILEGE...48

A. State Secrets Are Not Necessary To Establish Plaintiffs' Injury In Fact 49

B. State Secrets Are Not Necessary To Establish Causation 51

C. Plaintiffs May Take Discovery To Further Establish Standing............................52

V. SUMMARY JUDGMENT IS PREMATURE ON THIS RECORD................................52

A. The State Secrets Privilege Applies Only To Concrete Evidentiary Disputes And Should Not Be Applied Prematurely 52

B. The Government Must Provide A Reasonable Explanation For The Specific Basis Of Its Assertion Of The State Secrets Privilege On The Public Record Before Summary Judgment Could Be Appropriate 55

C. Congress Has Provided For Discovery In Electronic Surveillance Cases............56

D. Specific Non-Secret Discovery Should Proceed..57

CONCLUSION...58

TABLE OF AUTHORITIES

CASES **Page**

ACLU Found. of S. Cal. v. Barr,
952 F.2d 457 (D.C. Cir. 1991) 24

Anderson v. Liberty Lobby,
477 U.S. 242 (1986) 29

Anhydrides & Chemicals, Inc. v. United States,
130 F.3d 1481 (Fed. Cir. 1997) 23

Ashcroft v. ACLU,
542 U.S. 656 (2004) 39

Bd. of Educ. v. Earls,
536 U.S. 822 (2002) 43

Berger v. N.Y.,
388 U.S. 41 (1967) 37, 38, 39, 50

Black v. U.S.,
900 F. Supp. 1129 (D. Minn. 1994) 10, 11, 28, 47

Bosaw v. Nat'l Treasury Employees Union,
887 F. Supp. 1199 (S.D. Ind. 1995) 10

Burgert v. Lokelani Bernice Pauahi Bishop Trust,
200 F.3d 661 (9th Cir.2000) 28

Burlington N. & Santa Fe Ry. Co. v. The Assiniboine,
323 F.3d 767 (9th Cir. 2003); 57

Capital Cities Media, Inc. v. Toole,
463 U.S. 1303 (1983) 29

City of Indianapolis v. Edmond,
531 U.S. 32 (2000); 43

City of Milwaukee v. Ill.,
451 U.S. 304 (1981); 17

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 44

County of Oneida v. Oneida Indian Nation,
470 U.S. 226 (1985) 17

Dep't of the Navy v. Egan,
484 U.S. 518 (1988) 17

Dorfmont v. Brown,
913 F.2d 1399 (9th Cir. 1990) 17

DTM Research L.L.C. v. A.T.&T. Corp.,
245 F.3d 327 (4th Cir. 2001) 53

TABLE OF AUTHORITIES

Ecological Rights Found. v. Pacific Lumber Co.,
230 F.3d 1141 (9th Cir. 2000) 50

Edmond v. U.S.,
520 U.S. 651 (1997) 25

Edmunds v. U.S. DOJ,
323 F. Supp. 2d 65 (D.C.C. 2004) 16

Elkins v. U.S.,
364 U.S. 206 (1960) 26

Ellsberg v. Mitchell,
709 F.2d 51 (D.C. Cir. 1983), ... 28, 53, 54, 55

El-Masri v. Tenet,
2006 WL 1391390 (E.D. Va. May 12, 2006) 15

FDA v. Brown & Williamson Tobacco Corp.,
529 U.S. 120 (2000) 25

FEC v. Akins,
524 U.S. 11 (1998) 51, 52

Fitzgerald v. Penthouse Int'l, Ltd.,
776 F.2d 1236 (4th Cir. 1985) 14, 54

Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.,
204 F.3d 149 (4th Cir. 2000) 50, 51

Halkin v. Helms,
598 F.2d 1 (D.C. Cir. 1978) 39, 54

Halkin v. Helms,
690 F.2d 977 (D.C. Cir. 1982) 39, 54

Halperin v. Kissinger,
807 F.2d 180 (D.C. Cir. 1986) 22, 40

Halpern v. U.S.,
258 F.2d 36 (2d Cir. 1958) 19, 46, 54

Hamdi v. Rumsfeld,
542 U.S. 507 (2004) 26, 27

Heine v. Raus,
399 F.2d 785 (4th Cir. 1968) 53

Illinois v. McArthur,
531 U.S. 326 (2001) 42

In re Grand Jury Subpoena Dated Aug. 9, 2000,
218 F. Supp. 2d 544 (S.D.N.Y. 2002) 12

TABLE OF AUTHORITIES

In re Sealed Case,
310 F.3d 717 (U.S. F.I.S. Ct. Rev. 2002) 42

In re State Police Litigation,
888 F. Supp. 1235 (D. Conn. 1995) 32

In re Under Seal,
945 F.2d 1285 (4th Cir. 1991) 11, 52, 53

In re United States,
872 F.2d 472 (D.C. 1989) 10, 53

Int'l Indus. v. E.I. Dupont de Nemours & Co.,
140 F.R.D. 275 (S.D.N.Y. 1991) 30

Katz v. U.S.,
389 U.S. 347 (1967) 37

Kasza v. Browner,
113 F.3d 1159 (9th Cir. 1998) .... passim

Kinoy v. Mitchell,
67 F.R.D. 1 (S.D.N.Y. 1975) 55

Konop v. Hawaiin Airlines,
302 F.3d 868 (9th Cir. 2002) 32

Legal Services Corp. v. Velazquez,
531 U.S. 533 (2001) 28

Linder v. Nat'l Security Agency,
94 F.3d 693 (D.C. Cir. 1996) 52

Loral Corp. v. McDonnell Douglas Corp.,
558 F.2d 1130 (2nd Cir. 1977) 54

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 49, 51, 52

Marbury v. Madison,
5 U.S. 137 (1803) 26

McGehee v. Casey,
718 F.2d 1137 (D.C. Cir. 1983) 29

Metabolife Int'l v. Wornick,
264 F.3d 832 (9th Cir. 2001) 57

Mich. Dep't of State Police v. Sitz,
496 U.S. 444 (1990) 43

Molerio v. FBI,
749 F.2d 815 (D.C. Cir. 1984) 12, 28, 52

TABLE OF AUTHORITIES

Monarch Assur. P.L.C. v. U.S.,
244 F.3d 1356 (Fed. Cir. 2001) 10

New Jersey v. T.L.O.,
469 U.S. 325 (1985) 42

Nat'l Treasury Employees Union v. Von Raab,
489 U.S. 656 (1989) 43

Northrop Corp. v. McDonnel Douglas Corp.,
751 F.2d 395 (D.C. Cir. 1984) 52

Osborn v. U.S.,
385 U.S. 323 (1966). 38

Raines v. Byrd,
521 U.S. 811 (1997) 51

Reiter v. Sonotone Corp.,
442 U.S. 339 (1979) 20

Skinner v. Ry. Labor Executives' Ass'n,
489 U.S. 602 (1989) 43

Spock v. U.S.,
464 F. Supp. 510 (S.D.N.Y. 1978) 29, 54

Sterling v. Tenet,
416 F.3d 338 (4th Cir. 2005) 13, 15

Tenet v. Doe,
544 U.S. 1 (2005) 16

Tilden v. Tenet,
140 F. Supp. 2d 623 (E.D. Va. 2000) 53

Totten v. U.S.,
92 U.S. 105 (1875) .... passim

U.S. v. Martinez-Fuerte,
428 U.S. 543 (1976) 42

U.S. v. Reynolds,
345 U.S. 1 (1953) 10, 12

United States v. Belfield,
692 F.2d 141 (D.C. Cir. 1982) 24

United States v. Councilman,
418 F.3d 67 (1st Cir. 2005) 32

United States v. Estate of Romani,
523 U.S. 517 (U.S. 1998) 25

TABLE OF AUTHORITIES

United States v. Miller,
688 F.2d 652 (9th Cir. 1982) 44

United States v. Nixon,
418 U.S. 683 (1974) 12

United States v. Rodriguez,
968 F.2d 130 (2d Cir. 1992) 32

United States v. U.S. Dist. Ct. (Plamondon),
407 U.S. 297 (1972) 38, 40

United States v. Walther,
652 F.2d 788 (9th Cir.1981) 44

Vernonia School Dist. 47J v. Acton,
515 U.S. 646 (1995) 43

VISA Int'l Serv. Ass'n v. Bankcard Holders of Am.,
784 F.2d 1472 (9th Cir. 1986) 57

Webster v. Doe,
486 U.S. 592 (1988) 27

Williamson v. Gen. Dynamics Corp.,
208 F.3d 1144 (9th Cir. 2000) 28

Youngstown Sheet & Tube v. Sawyer,
343 U.S. 579 (1952) 22

Zuckerbraun v. General Dynamics Corp.,
935 F.2d 544 (2d Cir. 1991) 10, 14

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 39

STATUTES

5 U.S.C. § 102 .... 6, 24, 25

5 U.S.C. § 105 6

18 U.S.C. § 2510 18

18 USC § 2511(1)(a) 31

18 U.S.C. § 2511(2)(a)(ii) .... passim

18 U.S.C. § 2511(2)(f) 17, 18

18 U.S.C. § 2511(3) (1976) 34

18 U.S.C. § 2520 .... 18, 51

18 U.S.C. § 2701 18

TABLE OF AUTHORITIES

18 U.S.C. § 2702 .... 36, 37
18 U.S.C. § 2703(e) 18
18 U.S.C. § 2712(a) 22
18 U.S.C. § 3121 18
42 U.S.C § 6001 16
47 U.S.C. § 605(e)(3)(A) 19, 35
50 U.S.C. § 402 24
50 U.S.C. § 403-1(i)(1) 25
50 U.S.C. § 1801 18
50 U.S.C. § 1801(f)(2) 33
50 U.S.C. § 1801(n) 56
50 U.S.C. § 1801(l) 33
50 U.S.C. § 1802(b) 18
50 U.S.C. § 1806(f) .... passim
50 U.S.C. § 1809(a)(1) 33
50 U.S.C. § 1810 .... 18, 32, 51
50 U.S.C. § 1825(g) 17, 21, 22
50 U.S.C. § 1845(f) .... passim
50 U.S.C. § 2712(b)(4) 22

OTHER AUTHORITIES

H.R. Conf. Rep. No. 95-1720,
1978 U.S.C.C.A.N. 4048 (Oct. 5, 1978) 21, 22, 24
S. Rep. No. 95-604(I) (1978) 41
S. Rep. No. 95-701 (1978) 41

RULES

Fed. R. Civ. P. 56(f) 57

INTRODUCTION

For at least the past three years, AT&T has engaged in the wholesale illegal interception and disclosure to the NSA of its customers' personal communications and records. These actions violate no less than four federal statutes, each of which provides for a civil cause of action for illegal surveillance. They have been undertaken without regard to the judicially-controlled processes for supervising the executive's need to protect national security. And they do not constitute state secrets. For even without the benefit of the ordinary judicial discovery processes, plaintiffs have already presented a *prima facie* case on each cause of action using admittedly non-classified evidence.

Yet despite the settled statutory framework and the private rights of action established by Congress, and notwithstanding the non-secret record evidence supporting those claims, the government alleges that this case should be dismissed at the outset, pushing the common law "state secrets privilege" beyond all previous boundaries. To justify this broad expansion of executive power, the government must misstate what this case is actually about. Plaintiffs here do not seek information concerning how or why the NSA selects intelligence targets. Nor do they seek the details of how the NSA engages in its widely publicized data-mining of telephone and email records. Rather, the claims at issue here arise from a few very simple and non-classified facts.

Contrary to the government's contentions, AT&T's participation in surveillance activities is simply not a state secret. At AT&T's [redacted] Facility, for example, internet traffic arrives at the [redacted] Room through a fiber-optic cable. In that room, a copy of the internet traffic that AT&T receives – email, web browsing requests, and other electronic communications sent to or from the customers of AT&T's WorldNet Internet service – is diverted onto a separate fiber-optic cable through the use of a "[redacted]." The cabinet in turn is then connected to equipment in a special room, called the [redacted] Room. The [redacted] room was created under the supervision of the NSA, contains powerful computer equipment capable of analyzing large volumes of data and connecting to separate networks, distinct from the commercial AT&T network. Only personnel with NSA clearances – people assisting or acting on behalf of the NSA – have access to the [redacted] Room.

These acts constitute "interception" in violation of Title III of the Communications Act of 1934, and improper "electronic surveillance" in violation of the Foreign Intelligence Surveillance Act of 1978 ("FISA"). And when AT&T intercepted for the government Plaintiffs' and class members' communications without a warrant, it violated the Fourth Amendment of the United States Constitution. What the government did with that internet traffic after it was delivered by AT&T is not a necessary element of, or even particularly relevant to, Plaintiffs' claims.

These facts are not classified. Many of Plaintiffs' claims here are supported by evidence that has already been established to be beyond the ambit of the state secrets privilege: the testimony and documents of Mark Klein, a former AT&T technician who was not employed by the government and had no security clearance from the NSA, and the analysis of that evidence by former Senior Advisor for Internet Technology at the FCC, J. Scott Marcus. On March 30, 2006, the government was given an opportunity to review Mr. Klein's materials to evaluate whether to object to their use in this litigation. Far from invoking the state secrets privilege to cover those materials, the government instead allowed Plaintiffs to go forward. The government cannot unring that bell.

Plaintiffs have further alleged that AT&T also violated its customers' rights by turning over the customer detail records from its "Daytona" database system. When it did so, AT&T engaged in a "disclosure" also barred by, *inter alia,* the Stored Communication Act. Plaintiffs have also alleged warrantless surveillance of purely domestic telephone communications. As set forth in Section V, discovery corroborating these highly publicized events, which have not been denied by key government sources, can proceed without endangering state secrets.

Not only can Plaintiffs make their case without implicating the state secrets privilege, but AT&T can also defend itself – if it has a *bona fide* defense – without endangering state secrets. Congress has provided that if AT&T really did act with a valid government "authorization," then such an authorization cannot be cloaked as a "state secret" in order to dismiss this case. To do so would grant AT&T a blank check to continue or even expand the illegal surveillance and render illusory the private rights of action that Congress enacted as part of FISA, rights that Congress enacted in response to perceived abuses of the use of electronic surveillance conducted for national security. Alternatively, to the degree that confidentiality might attach to some aspect of such a certification, Congress has enacted laws that render them discoverable subject to appropriate safeguards.

The government's contention that this case should be dismissed and/or summarily adjudicated on the basis of the state secrets privilege is therefore flawed for five reasons.

First, absent truly exceptional circumstances (inapplicable here), the state secrets privilege constitutes a narrow evidentiary common law privilege and not an immunity from suit. In the area of electronic surveillance Congress has specifically limited the applicability of the state secrets privilege by statute. This common law privilege cannot render the Court powerless to review the violation by a civil defendant of eavesdropping and electronic surveillance laws passed by Congress. Nor does this common law privilege shield massive violations of the Fourth Amendment by the country's largest telecommunications company from judicial scrutiny and redress. *See* Section I.

Second, a close examination of the elements of proof required by Plaintiffs' claims demonstrates that the case does not turn on state secrets. On the contrary, these claims are fully supported by the government's existing admissions, by the Klein testimony and documents, and by Plaintiffs' expert, J. Scott Marcus. The government simply cannot repossess information that is already of record and transform it into a state secret. Nor should the government be permitted to evade judicial review by inaccurately recharacterizing Plaintiffs' claims as requiring proof of state secrets. *See* Section II.

Third, the statutory scheme bars the government from contending that the state secrets privilege can prevent disclosure of any alleged certification provided to AT&T – and as a corollary proposition that this case must be dismissed. As noted, that contention effectively nullifies the private rights of action Congress created to regulate electronic surveillance.

Moreover, the government's contention regarding the secret status of the certification defense is particularly meritless given the facts of this case. The only reason that the government and AT&T have asserted to bar disclosure of the possible certifications is that the existence or non-existence of a certification would tend to prove or disprove whether AT&T was involved in the alleged surveillance activities. That argument falls flat for the simple reason that AT&T's actions in divulging its customers' communications to the NSA are already set forth in non-secret record evidence.

Fourth, given the breadth of AT&T's violations of law there is no doubt that Plaintiffs have standing to assert their claims. AT&T engaged in a wholesale disclosure of customer information. AT&T cannot now contend that no individual customer has standing because it has inflicted an injury on all of them. Nor does the state secrets privilege bar the discovery of information pertinent to standing; indeed, the core facts are already of record. *See* Section IV.

Finally, summary judgment is plainly premature. Before such a procedure would be appropriate, the government must articulate with specificity why the privilege pertains to specific categories of information. The state secrets privilege could then be applied to concrete disputes, as the law requires. In the meantime, non-privileged discovery should proceed. Beyond the record already established, Plaintiffs are empowered by express statutory provisions to take further discovery in support of their claims. *See* Section V.

The government's proposition that this Court must summarily dismiss a case that is based upon non-secret evidence alleging a broad violation of fundamental constitutional rights of millions of American citizens is extraordinary, and extraordinarily dangerous. It seeks to use a common law evidentiary privilege to eliminate private rights of action created by Congress specifically to redress improper telecommunications surveillance. And it seeks to bar judicial review of a key constitutional question – the application of the Fourth Amendment to untargeted, ongoing surveillance of the private communications of millions of non-suspect Americans.

The Executive cannot deprive the Court of the ability to enforce these rights. The state secrets privilege overwrites neither the Constitution nor the express statutory scheme created by Congress. The government's assertion that it does should be denied.

STATEMENT OF FACTS

The record assembled by Plaintiffs on their pending motion for preliminary injunction – without any formal discovery – establishes the existence of a massive surveillance campaign by AT&T of email communications crossing its network. The declarations of Mark Klein and expert J. Scott Marcus establish the following key facts.

The Creation Of The [redacted] Room

Around January 2003, AT&T built a room at its [redacted] facility in San Francisco, subject to heightened security and accessible only to those with a clearance from the NSA. Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction, Dated March 28, 2006 ("Klein Decl."), ¶ 12 and Exs. A-C. The NSA was deeply involved in this process. While Mr. Klein was working at AT&T's [redacted] office in San Francisco, an NSA agent met with and interviewed a Field Support Specialist for a "special job" at the [redacted] Facility. Klein Decl., ¶ 10. In January 2003, Mr. Klein personally observed the construction of the [redacted] Room, which was nearing completion. *Id.*, ¶¶ 11-14. At that time he learned that the field support specialist was working to install equipment in the [redacted] Room. *Id.*, ¶ 14.

NSA Control Of The [redacted] Room

In October 2003, Mr. Klein was transferred to the [redacted] Facility, where his job was to oversee the [redacted] Room as a communications technician. Klein Decl., ¶ 15. In that room, communications carried by AT&T's WorldNet Internet service are directed to or from customers. Klein Decl., ¶ 19. Although Mr. Klein had keys to every other door at the [redacted] Facility, he did not have access to the [redacted] Room. *Id.*, ¶ 17. The regular AT&T technician workforce was not allowed in the [redacted] Room, which [redacted]. *Id.*, ¶ 17.

Only AT&T employees with NSA clearances had access to the [redacted] Room. Klein Decl., ¶ 17; *see also* ¶¶ 10, 14, 16-18. Executive Order No. 12968 governs NSA clearances. *See* Declaration of Michael M. Markman, filed herewith ("Markman Decl."), Ex. 1. It discusses clearance for "employees," which it defines to include all persons, whether employed by NSA or by a third party, "who act[s] for or on behalf of an agency as determined by the appropriate agency head." Exec. Order No. 12968 § 1.1(e) (1995) (emphasis added).[1] Thus, the AT&T employees cleared by the NSA act "**on behalf of the NSA**".

The Executive Order also requires that anyone granted access to classified information must have a demonstrated "need-to-know" in order to perform a governmental function. Exec. Order No. 12968 § 1.2(a) (1995), Markman Decl., Ex. 1. Absent special circumstances, eligibility also requires a demonstrated "need for access." *Id.*, § 2.1(b)(2). The regulation defines "need for access" and "need to know" in Section 1.1:

> "Need for access" means a determination that an employee requires access to a particular level of classified information in order **to perform or assist in a lawful and authorized governmental function**.
>
> "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information **in order to perform or assist in a lawful and authorized governmental function**.

Id., §§ 1.1(g) and (h) (emphasis added). Thus, the AT&T employees with NSA clearances to function within the [redacted] Room must, as a condition of their clearance, be performing or assisting in the performance of governmental functions.

The Communications Diverted To The [redacted] Room

AT&T connected fiber-optic cables in the [redacted] Facility's [redacted] Room to a "[redacted]." The cabinet diverted or copied the content of all of the electronic

---

[1] The Executive Order provides: "(a) 'Agency' means any 'Executive agency,' as defined in 5 U.S.C. 105, the 'military departments,' as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office."